



FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Egenevalueringsskjema

for foretakets IT-virksomhet

tilpasset eiendomsmeglingsforetak

Foretaksnavn:

Organisasjonsnummer:

Dato: 06.01.2020

Versjon 1.1

Finanstilsynet

Tlf. 22 93 98 00

post@finansstilsynet.no

www.finanstilsynet.no

Foretak:

Dato:

Underskrift:

Kontrollspørsmål - generelle	Ja	Nei	Kommen- tarer
1. Er foretaket kjent med at det er underlagt IKT-forskriften?			
2. Er foretaket kjent med innholdet i IKT-forskriften?			
3. Har foretaket sikret betryggende arkivering, gjenoppretting og sporbarhet av journaler ref. eiendomsmeglingsforskriften § 3.1?			
4. Har foretaket sikret betryggende arkivering, gjenoppretting og sporbarhet av regnskapsdata?			
5. Har foretaket sikret betryggende arkivering, gjenoppretting og sporbarhet av saksdokumenter ref. eiendomsmeglingsforskriften § 3.7?			
6. Er det etablert tiltak for å beskytte konfidensiell informasjon ved lagring og utveksling?			
7. Er det etablert tiltak som beskytter nettverk, systemer og data mot virus og andre typer ondsinnet kode?			
8. Er datamaskinene beskyttet mot bruk av andre enn ansatte?			
9. Er det i avtaler med leverandører av systemer og/eller IKT-driftstjenester sikret at krav til sikkerhet og leveranse kvalitet ivaretas?			
10. Er ulike krav til sikkerhet for IT-leverandører, som for eksempel taushetsplikt, identifisert og avtalt?			
11. Har foretaket etablert tiltak som sikrer at risikoanalyse av IT-virksomheten gjennomføres minst årlig og ved større endringer?			

12. Når ble siste risikoanalyse av IT-virksomheten gjennomført?			Dato:
13. Gjennomføres det testing av nye og endrede IT-løsninger?			
14. Foreligger det prosedyrer og kontroller for godkjenning av testresultater?			
15. Foreligger det en tilgjengelig kriseplan og er det etablert en prosedyre for oppdatering av denne?			
16. Blir det tatt regelmessig backup av data?			
17. Gjennomføres det testing av og øving i kriseløsningen og er resultatet dokumentert?			
18. Er det utarbeidet prosedyrer for håndtering av sikkerhetsbrudd og som beskriver hva som skal gjøres, for eksempel rapportering, eskalering og oppfølging?			

Kontrollspørsmål - tilgangsstyring	Ja	Nei	Kommentarer
1. Har foretaket dokumenterte retningslinjer for tilgangsstyring?			
2. Er retningslinjene basert på en rollebasert tilgangsstyring som beskriver typer tilganger, typer roller og hvilke roller som skal ha hvilke tilganger?			
3. Har foretaket utpekt hvem som er ansvarlige for tilgangstildelingen?			
4. Har foretaket dokumentert rutinene for hvordan tilgangsstyringen praktisk skal utføres?			
5. Omfatter rutinene for tilgangsstyring både oppretting, endring og sletting av tilganger?			
6. Beskriver rutinene for tilgangsstyring hva som er foretakets egne oppgaver og hva som er leverandøren(e)s oppgaver knyttet til utførelsen av tilgangsstyringen?			
7. Blir det gjennomført regelmessige gjennomganger av de ansattes tilgangsrettigheter?			
8. Bidrar leverandøren med uttrekk av lister som grunnlag for regelmessig gjennomgang av tilgangsrettighetene?			
9. Er det klarlagt i retningslinjene hvem som er ansvarlig for å iverksette og kontrollere resultatene av de regelmessige gjennomgangene?			
10. Ble siste rutinemessig kontroll av tilgangene gjennomført for mindre enn 12 måneder siden?			
11. Ble det funnet avvik som måtte korrigeres ved siste gjennomgang av tilgangene? I tilfelle ja, gi en kort beskrivelse.			